日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

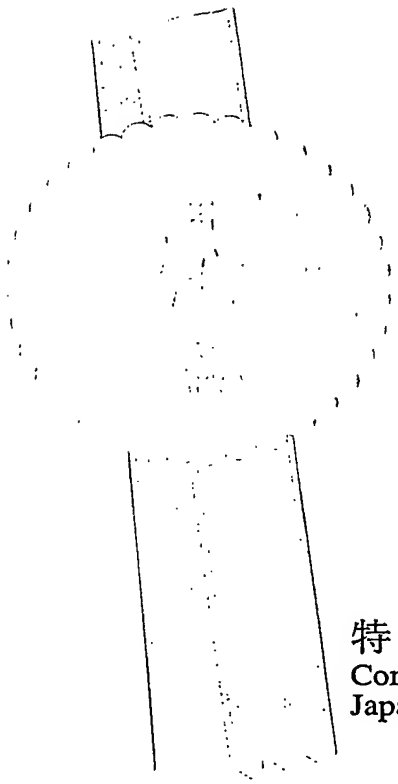
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　４月　４日

出願番号
Application Number: 特願２００３－１０１０８５

[ST. 10/C]: [ＪＰ２００３－１０１０８５]

出願人
Applicant(s): ＦＤＫ株式会社



２００３年１０月３１日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

【書類名】　特許願

【整理番号】　IP03527

【あて先】　特許庁長官　殿

【国際特許分類】　H03K　3/84

【発明者】

【住所又は居所】　東京都港区新橋５丁目３６番１１号　エフ・ディー・ケイ株式会社内

【氏名】　山本　博康

【発明者】

【住所又は居所】　東京都港区新橋５丁目３６番１１号　エフ・ディー・ケイ株式会社内

【氏名】　志賀　隆明

【発明者】

【住所又は居所】　東京都港区新橋５丁目３６番１１号　エフ・ディー・ケイ株式会社内

【氏名】　曽我　竜司

【発明者】

【住所又は居所】　東京都港区新橋５丁目３６番１１号　エフ・ディー・ケイ株式会社内

【氏名】　上遠野　昌良

【発明者】

【住所又は居所】　東京都港区新橋５丁目３６番１１号　エフ・ディー・ケイ株式会社内

【氏名】　渡邊　利幸

【特許出願人】

【識別番号】　000237721

【氏名又は名称】　エフ・ディー・ケイ株式会社

【代理人】

【識別番号】　100067046

【弁理士】

【氏名又は名称】　尾股　行雄

【電話番号】　03-3543-0036

【選任した代理人】

【識別番号】　100096862

【弁理士】

【氏名又は名称】　清水　千春

【電話番号】　03-3543-0036

【手数料の表示】

【予納台帳番号】　008800

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　物理乱数発生装置

【特許請求の範囲】

【請求項１】　物理乱数発生器を有する物理乱数発生装置であって、

前記物理乱数発生器が、

基準クロック信号に応じてシリアル乱数を生成するシリアル物理乱数発生器を備え、

シリアル乱数をパラレル乱数に変換するシリアル／パラレル変換部を備え、

パラレル乱数を保持しうる複数個のレジスターを備え、

前記シリアル／パラレル変換部によってパラレル乱数が生成される度に前記レジスターに順次パラレル乱数を保持し、かつ、読出しクロック信号に応じて前記レジスターからパラレル乱数を読み出して出力するとともに、読み出しの終了したレジスターに他のレジスターからパラレル乱数をシフトさせて内容を逐次更新する制御回路を備えたことを特徴とする物理乱数発生装置。

【請求項２】　前記物理乱数発生器が、

複数個のレジスターのうちパラレル乱数を保持すべきレジスターを決めて書き込みアドレスを出力するアップ／ダウンカウンターを備え、

前記アップ／ダウンカウンターが出力した書き込みアドレスに基づき、パラレル乱数を保持すべきレジスターを選択してロード信号を出力するセレクターを備え、

前記セレクターからのロード信号に基づいて前記シリアル／パラレル変換部内のパラレル乱数を前記レジスターのうち後段のレジスターから前段のレジスターへ順次保持し、かつ、読出しクロック信号に応じて前記レジスターのうち最後段からパラレル乱数を読み出して出力するとともに、このレジスターより前段にある各レジスター内のパラレル乱数を後段へ順次シフトする制御回路を備えたことを特徴とする請求項１に記載の物理乱数発生装置。

【請求項３】　前記物理乱数発生器が、

前記シリアル物理乱数発生器が生成したシリアル乱数の総数をカウントする総数カウンターを備え、

前記総数カウンターがカウントしたシリアル乱数の総数が所定のビット数に達したとき、これらのシリアル乱数に基づいてその一様性を検証する乱数検証回路を備えたことを特徴とする請求項１または請求項２に記載の物理乱数発生装置。

【請求項４】　前記乱数検証回路の乱数検証方法として、

乱数値“０”または“１”の出現度数をカウントし、これを規定値と比較することによって乱数の一様性を検証する乱数検証方法を採用したことを特徴とする請求項３に記載の物理乱数発生装置。

【請求項５】　前記乱数検証回路の乱数検証方法として、

４ビットで一つの乱数値とし、各々の乱数値の出現度数に基づいて算出されたχ二乗値を規定値と比較することによって乱数の一様性を検証する乱数検証方法を採用したことを特徴とする請求項３に記載の物理乱数発生装置。

【請求項６】　前記乱数検証回路の乱数検証方法として、

連の長さ別にその出現度数をカウントし、これらを規定値と比較することによって乱数の一様性を検証する乱数検証方法を採用したことを特徴とする請求項３に記載の物理乱数発生装置。

【請求項７】　前記乱数検証回路の乱数検証方法として、

所定ビット数の乱数中に出現した最長の連の長さを規定値と比較することによって乱数の一様性を検証する乱数検証方法を採用したことを特徴とする請求項３に記載の物理乱数発生装置。

【請求項８】　チップセレクトと出力イネーブル機能とそれに対応した端子を備え、出力部のバッファー機能を３ステートとしたことを特徴とする請求項１から請求項７までのいずれかに記載の物理乱数発生装置。

【請求項９】　前記物理乱数発生器を複数個用意し、セレクターのセレクト信号に基づき、前記物理乱数発生器の中から一つを選択して乱数または乱数検証データを出力するようにしたことを特徴とする請求項１から請求項８までのいずれかに記載の物理乱数発生装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、各種の用途に用いるに好適な物理乱数発生装置に関するものであり、その具体的な用途としては、セキュリティー、暗号、認証、施錠、暗号化通信、スマートカード（例えば、電子マネー、クレジットカード、診察券）、ホームセキュリティー、カーセキュリティー、キーレスエントリー、確率、抽選、ゲーム、アミューズメント（例えば、パチンコ、パチスロ）、シミュレーション（例えば、気象・学術計算・株価におけるモンテカルロ）、グラフィックス（例えば、ＣＧ、自動作曲）、制御、計測、ＦＡ、ロボット制御（人工知能）などが挙げられる。

【０００２】

【従来の技術】

従来この種の物理乱数発生装置としては、半導体内で発生するノイズを用いたものが多く、パソコンに外部から接続して使用するよう構成される規模の大きなものや、ＩＣチップ単体で乱数を発生させるものがあった。また、アミューズメント用には、時間的にランダムであると見なせる信号が発生した時に、備えられた高速カウンターの値を参照し、それを乱数として用いるものがあった。

【０００３】

【発明が解決しようとする課題】

一般に物理乱数発生器は高速に乱数を発生することは難しく、時としてその乱数発生速度以上の大量の乱数が必要となる事が起こる。そのため、記憶媒体を設けて乱数を貯めておいたり、複数の物理乱数発生装置を用いで乱数の発生量を増やしたりすることが考えられるが、これを実現するためには複雑な回路を利用者側で組む必要が生じる。

【０００４】

また、一般に物理乱数は使用環境によって乱数の質が変化する可能性があり、利用者がこれら物理乱数発生装置の発生した乱数が真正乱数として使用することができるか否かを確認することは有益なことである。しかしながら、乱数の検定を行うには専用の測定装置を構築しなければならず、一般の物理乱数発生装置利用者にとっては、このような余計なコストと手間がかかるような作業は受け入れ難い。また、乱数検定は大量のデータを扱うので、それを貯めておく記憶装置は

大容量のものが必要となるとともに、検定のための計算処理にも時間がかかる。

【０００５】

本発明は、このような事情に鑑み、物理乱数発生装置単体での乱数利用効率が高く、かつ複数の物理乱数ＩＣを組み上げて乱数を高速に発生させることが容易であり、さらに、乱数の質を容易に確認して使用することが可能な物理乱数発生装置を提供することを目的とする。

【０００６】

【課題を解決するための手段】

まず、本発明のうち請求項１に係る発明は、物理乱数発生器を有する物理乱数発生装置であって、前記物理乱数発生器が、基準クロック信号に応じてシリアル乱数を生成するシリアル物理乱数発生器を備え、シリアル乱数をパラレル乱数に変換するシリアル／パラレル変換部を備え、パラレル乱数を保持しうる複数個のレジスターを備え、前記シリアル／パラレル変換部によってパラレル乱数が生成される度に前記レジスターに順次パラレル乱数を保持し、かつ、読出しクロック信号に応じて前記レジスターからパラレル乱数を読み出して出力するとともに、読み出しの終了したレジスターに他のレジスターからパラレル乱数をシフトさせて内容を逐次更新する制御回路を備えて構成される。ここで、読出しクロックは基準クロックとは別に入力されるものである。

【０００７】

また、本発明のうち請求項２に係る発明は、前記物理乱数発生器が、複数個のレジスターのうちパラレル乱数を保持すべきレジスターを決めて書き込みアドレスを出力するアップ／ダウンカウンターを備え、前記アップ／ダウンカウンターが出力した書き込みアドレスに基づき、パラレル乱数を保持すべきレジスターを選択してロード信号を出力するセレクターを備え、前記セレクターからのロード信号に基づいて前記シリアル／パラレル変換部内のパラレル乱数を前記レジスターのうち後段のレジスターから前段のレジスターへ順次保持し、かつ、読出しクロック信号に応じて前記レジスターのうち最後段からパラレル乱数を読み出して出力するとともに、このレジスターより前段にある各レジスター内のパラレル乱数を後段へ順次シフトする制御回路を備えて構成される。

【０００８】

また、本発明のうち請求項３に係る発明は、前記物理乱数発生器が、前記シリアル物理乱数発生器が生成したシリアル乱数の総数をカウントする総数カウンターを備え、前記総数カウンターがカウントしたシリアル乱数の総数が所定のビット数に達したとき、これらのシリアル乱数に基づいてその一様性を検証する乱数検証回路を備えて構成される。

【０００９】

また、本発明のうち請求項４に係る発明は、前記乱数検証回路の乱数検証方法として、乱数値“０”または“１”の出現度数をカウントし、これを規定値と比較することによって乱数の一様性を検証する乱数検証方法を採用して構成される。

【００１０】

また、本発明のうち請求項５に係る発明は、前記乱数検証回路の乱数検証方法として、４ビットで一つの乱数値とし、各々の乱数値の出現度数に基づいて算出されたχ二乗値を規定値と比較することによって乱数の一様性を検証する乱数検証方法を採用して構成される。

【００１１】

また、本発明のうち請求項６に係る発明は、前記乱数検証回路の乱数検証方法として、連の長さ別にその出現度数をカウントし、これらを規定値と比較することによって乱数の一様性を検証する乱数検証方法を採用して構成される。

【００１２】

また、本発明のうち請求項７に係る発明は、前記乱数検証回路の乱数検証方法として、所定ビット数の乱数中に出現した最長の連の長さを規定値と比較することによって乱数の一様性を検証する乱数検証方法を採用して構成される。

【００１３】

また、本発明のうち請求項８に係る発明は、チップセレクトと出力イネーブル機能とそれに対応した端子を備え、出力部のバッファー機能を３ステートとして構成される。

【００１４】

さらに、本発明のうち請求項９に係る発明は、前記物理乱数発生器を複数個用意し、セレクターのセレクト信号に基づき、前記物理乱数発生器の中から一つを選択して乱数または乱数検証データを出力するようにして構成される。

【００１５】

【発明の実施の形態】

以下、本発明の実施形態を図面に基づいて説明する。

図１は本発明に係る物理乱数発生装置の第１の実施形態を示す回路図、

図２は図１に示す物理乱数発生装置の物理乱数発生器の詳細を示す回路図、

図３は図２に示す物理乱数発生器の各部の出力波形を示す波形図、

図４は図２に示す物理乱数発生器の各部の出力波形を示す波形図、

図５は図１に示す物理乱数発生装置の乱数検証回路のMonobitTestに関する部分の回路図、

図６は図１に示す物理乱数発生装置の乱数検証回路のPokerTestに関する部分の回路図、

図７は図１に示す物理乱数発生装置の乱数検証回路のRunsTestに関する部分の回路図、

図８は図１に示す物理乱数発生装置の乱数検証回路のRunsTestに関する部分の回路図、

図９は図１に示す物理乱数発生装置の乱数検証回路のLongRunsTestに関する部分の回路図である。

【００１６】

この物理乱数発生装置９１は、図１に示すように、物理乱数発生器１、乱数検証回路２１、制御回路９４、カウンター９５、第１セレクター９６、第２セレクター９７から構成されており、物理乱数発生器１は、図２に示すように、シリアル物理乱数発生器２、カウンター３、シフトレジスター４、複数個（図２ではm個）のレジスター５、制御回路６、アップ／ダウンカウンター７、セレクター８、基準クロック側の２個の遅延回路９および読出しクロック側の２個の遅延回路１０から構成されている。

【００１７】

他方、乱数検証回路２１は、図５から図９までに示すように、乱数検定規格ＦＩＰＳ１４０－２に準拠した４種類の検定方法（MonobitTest、PokerTest、Runs TestおよびLongRunsTest）に対応する部分から構成されている。すなわち、MonobitTestに関する部分は、図５に示すように、第１カウンター２３、第２カウンター２４、レジスター２５、制御回路２６および比較器２７から構成されており、PokerTestに関する部分は、図６に示すように、第１カウンター３３、シフトレジスター３４、デコーダー３５、複数個（図６では１６個）のカウンター３６、制御回路３７、セレクター３８、掛算器３９、加算器４０、レジスター４１および比較器４２から構成されている。また、RunsTestに関する部分はさらに乱数出力が“１”の場合と乱数出力が“０”の場合とに二分され、前者は、図７に示すように、第１カウンター５３、比較器５４、データ保持器５５、第２カウンター５６、制御回路５７、デコーダー５８、６個のカウンター５９および６個の比較器６０から構成されており、後者は、図８に示すように、物理乱数発生器１のシリアル物理乱数発生器２からデコーダー５８への出力線上にインバータが設けられて出力が反転する点を除き、前者と同じ構成を有している。さらに、LongRunsTestに関する部分は、図９に示すように、第１カウンター７３、比較器７４、データ保持器７５、制御回路７６、第２カウンター７７、第１比較器７８、レジスター７９および第２比較器８０から構成されている。

【００１８】

物理乱数発生装置９１は以上のような構成を有するので、この物理乱数発生装置９１を作動させると、まず物理乱数発生器１で、シリアル乱数が出力されるとともに、パラレル乱数が保持されて必要に応じて出力できる状態となる。

【００１９】

すなわち、基準クロック(CLK_0)でシリアル物理乱数発生器２より生成されたシリアル乱数(SRND)をカウンター３のキャリーアウト(CO)に同期して、シフトレジスター４でシリアルからパラレルに変換したｎビットの乱数(CRND)をセレクター８で選択されたレジスター５にロードしてパラレル乱数を保持する。

【００２０】

このとき、セレクター８はアップ／ダウンカウンター７の出力の書込みアドレ

ス(ADDRESS)で指定されたレジスター５を選択し、カウンター３のキャリーアウト(CO)に同期してパラレル乱数(CRND)をレジスター５にロードし、ロードごとにアップ／ダウンカウンター７をカウントアップし、アップ／ダウンカウンター７の出力の書込みアドレス(ADDRESS)がｍになった時点で、アップ／ダウンカウンター７はカウントアップとパラレル乱数のロードを中止し、以降その状態を維持する。

【００２１】

パラレル乱数の出力(PRND)は最下位のレジスター５の出力とし、読み出し後に読出しクロック(CLK_R)を入力し、読出しクロックにてアップ／ダウンカウンター７のカウントダウンとすべてのレジスター５内のデータを上位から下位へシフトし、パラレル乱数(PRND)はその都度更新される。アップ／ダウンカウンター７の出力の書込みアドレス(ADDRESS)がゼロになった時点で、アップ／ダウンカウンター７はカウントダウンとデータシフトを中止し、以降その状態を維持する。

【００２２】

アップ／ダウンカウンター７の出力の書込みアドレス(ADDRESS)は外部に出力され、すべてのレジスター５に保持されているパラレル乱数の数を逐次モニター可能とする。

【００２３】

遅延回路９、１０は各クロックのエッジ（例えば、立上りエッジ）を取り出し、非常に短いパルス波形（例えば、１０ｎｓ）を生成し、アップ／ダウンカウンター７とすべてのレジスター５のクロック信号(CLOCK)、アップ／ダウンカウンター７のENABLE信号、すべてのレジスター５のSHIFT信号とLOAD(0)～LOAD(m-1)を生成する。これにより、基準クロック(CLK_0)と読出しクロック(CLK_R)が非同期または同期式で動作するときに、基準クロック(CLK_0)のエッジ（例えば、立上りエッジ）に対する読出しクロック(CLK_R)のエッジ（例えば、立上りエッジ）の禁止域(td_Ra+td_0a+２×td_mg)を非常に小さくして基準クロック(CLK_0)と読出しクロック(CLK_R)との干渉を最小限とすることができる。なお、CLK_0bとCLK_Rbがクロック信号(CLOCK)を生成し、CLK_0aとCLK_RaがENABLE信号、SHIFT信号とLOAD(0)～LOAD(m-1)を生成する。

【００２４】

制御回路６はカウンター３のキャリーアウト(CO)の同期信号(SYNC)、CLK_0a、CLK_Ra、アップ／ダウンカウンター７のOVER信号とZERO信号より、アップ／ダウンカウンター７のUP/DOWN信号とENABLE信号、すべてのレジスター５のSHIFT信号とLOAD(0)～LOAD(m-1)用のLOAD信号を生成する。

【００２５】

こうすることにより、基準クロックに同期してシリアル物理乱数発生器２で生成されたシリアル乱数よりｎ倍の周期で最大ｍ個のｎビットのパラレル乱数を保持することができる。それ以降のシリアル乱数は読み出し操作（CLK_Rの入力）をするまでは保持されない。こうして保持された最大ｍ個のパラレル乱数は読出しクロックで必要なときに必要な量（最大ｍ個）を短時間に集中して読み出すことができ、読み出された量のパラレル乱数は逐次補充される。基準クロック(CLK_0)のエッジに対する読出しクロックのエッジの禁止域が非常に狭く、非同期または同期式でタイミングよく、かつ効率的に読み出すことができる。書込みアドレスを読み出すことで、その時点で保持されたパラレル乱数の量を確認することが可能となり、乱数を効率的に活用することができる。

【００２６】

ところで、こうしてシリアル物理乱数発生器２で生成されたシリアル乱数は、乱数検定規格ＦＩＰＳ１４０－２に準拠した４種類の検定方法（MonobitTest、PokerTest、RunsTestおよびLongRunsTest）でその一様性が検証される。

【００２７】

まず、MonobitTestによる検証が行われる。すなわち、図５に示すように、第１カウンター２３はスタート信号(START)と基準クロック(CLK_0)より制御回路２６を介して生成された信号START_Cでカウントを開始し、20,000カウント時に信号OUT_Cを出力する。第２カウンター２４は制御回路２６の出力信号CLR_C2でスタート信号(START)が入った時点に初期化を行い、シリアル乱数(SRND)の“１”または“０”をカウントする。レジスター２５は制御回路２６の出力信号LOAD_Rでスタート信号(START)が入った時点より20,000クロック時の第２カウンター２４のカウント値をロードして保持し、MonobitData(MOND)を出力する。比較器２

７はレジスター２５の出力MonobitData(MOND)と上限比較データ（例えば、10,275bit）および下限比較データ（例えば、9,725bit）とを比較し、MonobitJudge(MONJ)信号を出力する。これにより、基準クロックに同期して生成されたシリアル乱数について、スタート信号から20,000クロック後にMonobitDataとMonobitJudgeを検証することができる。

【００２８】

次に、PokerTestによる検証が行われる。すなわち、図６に示すように、第１カウンター３３はスタート信号(START)と基準クロック(CLK_0)より制御回路３７を介して生成された信号START_Cでカウントを開始し、20,000カウント時に信号OUT_Cを出力する。シフトレジスター３４はシリアル乱数(SRND)を基準クロック(CLK_0)にて逐次４ビットのパラレル乱数(PRND_4B)に変換する。デコーダー３５は、スタート信号(START)と基準クロック(CLK_0)より制御回路３７を介して生成されたENABLE信号がアクティブのとき（４クロックごとに１回）にパラレル乱数(PRND_4B)で指定された出力部(SE_0～SE_15)に出力される。カウンター３６は制御回路３７の出力信号CLR_CRでスタート信号(START)が入った時点に初期化を行い、ENABLE信号がアクティブのとき（４クロックごとに１回）にパラレル乱数(PRND_4B)のデータにてデコーダー３５で指定されたカウンター３６をカウントアップする。すべてのカウンター３６の総計は5,000カウントとなり、基準クロックに同期して生成されたシリアル乱数について、スタート信号から20,000クロック後にその間の４ビットごとのパラレル乱数(PRND_4B)のデータ（０～１５）の度数分布データ(PokerData0～PokerData15)を取得する。レジスター４１は、制御回路３７の出力信号CLR_CRでスタート信号(START)が入った時点に初期化(POKD=0)を行い、度数分布データ(PokerData0～PokerData15)を取得した後、セレクター３８、掛算器３９、加算器４０を介して度数分布データ(PokerData0～PokerData15)の１６個の二乗和を求めることでPokerData(POKD)を取得する。比較器４２はレジスター４１の出力PokerData(POKD)と上限比較データ（例えば、1,576,928）および下限比較データ（例えば、1,563,175）とを比較し、PokerJudge(POKJ)信号を出力する。これにより、基準クロックに同期して生成されたシリアル乱数について、スタート信号から20,000+16クロック後にPokerDataとPokerJudgeを検証

することができる。

【００２９】

次いで、RunsTestによる検証が行われる。すなわち、図７および図８に示すように、第１カウンター５３はスタート信号(START)と基準クロック(CLK_0)より制御回路５７を介して生成された信号START_Cでカウントを開始し、20,000カウント時に信号OUT_Cを出力する。データ保持器５５はシリアル乱数(SRND)を基準クロック(CLK_0)にて逐次１ビット保持し、比較器５４はシリアル乱数(SRND)とデータ保持器５５で保持された乱数を比較し、１クロック前の乱数と今回の乱数が変化したときに信号CHANGEを出力する。第２カウンター５６は、信号CHANGEが出力されてから次の出力がされるまでのクロックをカウントし、信号RUNS_Dを出力する。信号RUNS_Dと同一信号の長さ(L)の関係はL=RUNS_D+1となる。第２カウンター５６は、制御回路５７の出力信号CLR_CCでスタート信号(START)が入ったときと信号CHANGEが出力されたときに初期化(RUNS_D=0)を行う。デコーダー５８は、スタート信号(START)、基準クロック(CLK_0)、第１カウンター５３の出力(OUT_C)と比較器５４の出力(CHANGE)より制御回路５７を介して生成されたENABLE信号がアクティブ（CHANGEがアクティブ）のときで、図７ではシリアル乱数(SRND)が“１”のとき、図８ではシリアル乱数(SRND)が“０”のとき、第２カウンター５６の出力(RUNS_D)で選択された出力(SE_1～SE_6+)をアクティブにする。なお、L=1→SE_1、L=2→SE_2、…、L=6+→SE_6+となる。すべてのカウンター５９は、制御回路５７の出力信号CLR_Cでスタート信号(START)が入った時点に初期化を行い、デコーダー５８の出力(SE_1～SE_6+)で指定されたカウンター５９をカウントアップし、１～６＋の同一信号の長さ(L)の出現回数（図７ではRunsData1H～RunsData6+H、図８ではRunsData1L～RunsData6+L）を取得する。各比較器６０は各カウンター５９の出力（図７ではRunsData1H～RunsData6+H、図８ではRunsData1L～RunsData6+L）とそれぞれの上限比較データ（例えば、2,685、1,386、723、384、209、209）および下限比較データ（例えば、2,315、1,114、527、240、103、103）とを比較し、判定信号（図７ではRunsJudge1H～RunsJudge6+H、図８ではRunsJudge1L～RunsJudge6+L）を出力する。これにより、基準クロックに同期して生成されたシリアル乱数について、スタート信号から20,000クロック後に

RunsTestのデータと判定を検証することができる。

【００３０】

最後に、LongRunsTestによる検証が行われる。すなわち、図９に示すように、第１カウンター７３はスタート信号(START)と基準クロック(CLK_0)より制御回路５７を介して生成された信号START_Cでカウントを開始し、20,000カウント時に信号OUT_Cを出力する。データ保持器７５はシリアル乱数(SRND)を基準クロック(CLK_0)にて逐次１ビット保持し、比較器７４はシリアル乱数(SRND)とデータ保持器７５で保持された乱数を比較し、１クロック前の乱数と今回の乱数が変化したときに信号CHANGEを出力する。第２カウンター７７は、信号CHANGEが出力されてから次の出力がされるまでのクロックをカウントし、信号LRUNS_Dを出力する。第２カウンター７７は、制御回路７６の出力信号CLR_CCでスタート信号(START)が入ったときと信号CHANGEが出力されたときに初期化(LRUNS_D=0)を行う。レジスター７９は、制御回路７６の出力信号CLR_Rでスタート信号(START)が入ったときに初期化(LRUNS_D=0)を行う。レジスター７９の出力信号LongRunsData(LRND)と第２カウンター７７の出力信号(LRUNS_D)を第１比較器７８で比較し、LRND＜LRUNS_Dのときに第１比較器７８は出力信号COMP_Uを出力し、制御回路７６を介してレジスター７９にLOAD_R信号を出力して、レジスター７９に逐次LRUNS_Dの最大値を保持する。第２比較器８０は上限比較データ（例えば、26）と比較し、判定信号LongRunsJudge(LRNJ)を出力する。信号LRUNS_D、LRNDと同一信号の長さ(L)の関係はL=LRUNS_D+1、L(max)=LRND+1=LRUNS_D(max)+1となる。これにより、基準クロックに同期して生成されたシリアル乱数について、スタート信号から20,000クロック後にLongRunsTestのデータと判定を検証することができる。

【００３１】

そして、こうして４種類の検定方法で検証された一様性乱数の検証データは、図１に示すように、第２セレクター９７に保持され、使用者の要望に応じて出力される。選択信号(A0、A1)と動作テーブルを表１に示す。

【表１】

ADDRE_S	A1	A0	読出しクロック(CLK_R)の働き	出力(DATA BUS)
0	0	0	パラレル物理乱数の更新	パラレル物理乱数
1	0	1	パラレル物理乱数の更新	パラレル物理乱数の生成状態
2	1	0	乱数検証のスタート／カウンターの初期化	乱数検証状態／モニターアドレス
3	1	1	乱数検証のモニターアドレス更新	乱数検証結果／検証データ

【００３２】

すなわち、物理乱数発生器１は、選択信号(A1)の状態（“０”または“１”）により、読出しクロック(CLK_R)でのパラレル乱数の更新（アップ／ダウンカウンター７のカウントダウン）または非更新とする。出力のパラレル乱数(PRND)は第２セレクター９７のDATA_0に接続される。出力(COND_R)には書込みアドレス(ADDRESS)などの物理乱数生成時およびパラレル乱数変換時に生成される各種データやフラグを出力し、第２セレクター９７のDATA_1に接続される。

【００３３】

乱数検証回路２１は、選択信号(A0、A1)が２(ADDRE_S)のときに制御回路９４を介して読出しクロック(CLK_R)信号で検証を開始し、MonobitTest、PokerTest、RunsTestおよびLongRunsTestを基準クロック(CLK_0)で20,000+16サイクルで完了し、判定結果、判定データ、PokerTestの生データを出力して第１セレクター９６に接続される。その詳細を表２に示す。

【表２】

ﾓﾆﾀｰｱﾄﾞﾚｽ(SEL_ADD)	出力(DATA BUS)
0	0 ; Monobit Judge(MONJ) 1 ; Poker Judge(POKJ) 2 ; Runs Judge 1H(RUNJ1H) 3 ; Runs Judge 1L(RUNJ1L) 4 ; Runs Judge 2H(RUNJ2H) 5 ; Runs Judge 2L(RUNJ2L) 6 ; Runs Judge 3H(RUNJ3H) 7 ; Runs Judge 3L(RUNJ3L) 8 ; Runs Judge 4H(RUNJ4H) 9 ; Runs Judge 4L(RUNJ4L) 10 ; Runs Judge 5H(RUNJ5H) 11 ; Runs Judge 5L(RUNJ5L) 12 ; Runs Judge 6+H(RUNJ6+H) 13 ; Runs Judge 6+L(RUNJ6+L) 14 ; Long Run Judge(LRNJ) 15 ; 総合判定
1	Monobit Data(MOND)
2	Poker Data(POKD)
3	Runs Data 1H(RUND1H)
4	Runs Data 1L(RUND1L)
5	Runs Data 2H(RUND2H)
6	Runs Data 2L(RUND2L)
7	Runs Data 3H(RUND3H)
8	Runs Data 3L(RUND3L)
9	Runs Data 4H(RUND4H)
10	Runs Data 4L(RUND4L)
11	Runs Data 5H(RUND5H)
12	Runs Data 5L(RUND5L)
13	Runs Data 6+H(RUND6+H)
14	Runs Data 6+L(RUND6+L)
15	Long Run Data(LRND)
16	Poker Data 0 (POK_0)
17	Poker Data 1 (POK_1)
18	Poker Data 2 (POK_2)
19	Poker Data 3 (POK_3)
20	Poker Data 4 (POK_4)
21	Poker Data 5 (POK_5)
22	Poker Data 6 (POK_6)
23	Poker Data 7 (POK_7)
24	Poker Data 8 (POK_8)
25	Poker Data 9 (POK_9)
26	Poker Data 10 (POK_10)
27	Poker Data 11 (POK_11)
28	Poker Data 12 (POK_12)
29	Poker Data 13 (POK_13)
30	Poker Data 14 (POK_14)
31	Poker Data 15 (POK_15)

【００３４】

なお、総合判定はすべての判定結果が合格のときに出力される。出力(COND_T)

には、乱数検証時に生成される各種データやフラグを出力し、第２セレクター９７のDATA_2にカウンター出力のモニターアドレス(SEL_ADD)とともに接続される。また、検証のスタート信号にてパラレル乱数生成用のカウンター３、シフトレジスター４、アップ／ダウンカウンター７とすべてのレジスター５は初期化され、検証された物理乱数を保持して検証後の物理乱数を使用することができる。

【００３５】

カウンター9.5は第１セレクター９６のモニターアドレス(SEL_ADD)を生成する。カウンター９５は、制御回路９４の出力信号(CLR_C)で選択信号(A0、A1)が２(ADDRE_S)のときに読出しクロック(CLK_R)信号で検証を開始し、この開始時に初期化を行い、制御回路９４の出力信号(CLK_C)で選択信号(A0、A1)が３(ADDRE_S)のときに読出しクロック(CLK_R)信号でカウンター９５のカウントアップ（更新）を行う。

【００３６】

これにより、基準クロックに同期して生成されたシリアル乱数(SRND)と逐次補充されるパラレル乱数(PRND)の生成および一様性の検証を逐次行うことができる。

【００３７】

こうすることにより、物理乱数発生器１の検証およびデータの確認が容易となり、検証後の乱数を活用することができる。選択信号(A0、A1)と第２セレクター９７を用いることで入出力端子を大幅に減らすことができる。選択信号(A0、A1)、読出しクロック(CLK_R)、カウンター９５と第２セレクター９７で、参照できる有効な検証データを拡大することができる。

【００３８】

なお、図１０に示すように、物理乱数発生器１にチップセレクト(CS)と出力イネーブル(OE)の入力を付加し、パラレル乱数[PRND(0)～PRND(n-1)]の出力形態を３ステート（“０”、“１”、off）にすることもできる。

【００３９】

また、図１１および図１２に示すように、複数個（図１１ではｐ個）の物理乱数発生器１とセレクター１２とで高速（図１１ではｐ倍）の乱数生成スピードを

獲得することも可能である。ここで、基準クロック(CLK_0)のエッジ（例えば、立上りエッジ）に対する読出しクロック(CLK_R)のエッジ（例えば、立上りエッジ）の禁止域(td_Ra+td_0a+２×td_mg)を非常に狭く考慮することのみで非同期または同期式の高速乱数発生を容易に実現することができる。

【００４０】

このように、チップセレクト(CS)と出力イネーブル(OE)を有することで、物理乱数発生器１を複数個接続することが容易となり、乱数生成の高速化が可能となる。また、チップセレクト(CS)と出力イネーブル(OE)を有することで、ＣＰＵを使用したシステムに物理乱数発生器１を容易に接続することができる。

【００４１】

なお、上述の実施形態では、基準クロック(CLK_0)のエッジに対する読出しクロック(CLK_R)のエッジの禁止域(td_Ra+td_0a+２×td_mg)を非常に小さくして基準クロック(CLK_0)と読出しクロック(CLK_R)との干渉を最小限とするため、基準クロック側および読出しクロック側にそれぞれ２個の遅延回路９、１０を設けた場合について説明したが、基準クロック側と読出しクロック側のいずれか一方にだけ遅延回路９、１０を設けてもよく、遅延回路９、１０の個数も１個以上であれば何個でも構わない。或いはまた、遅延回路９、１０に代えて波形成形回路（例えば、単安定マルチバイブレータ）を付加しても、同じ効果を得ることができる。

【００４２】

（付記１）物理乱数発生器を有する物理乱数発生装置であって、前記物理乱数発生器が、基準クロック信号に応じてシリアル乱数を生成するシリアル物理乱数発生器を備え、シリアル乱数をパラレル乱数に変換するシリアル／パラレル変換部を備え、パラレル乱数を保持しうる複数個のレジスターを備え、前記シリアル／パラレル変換部によってパラレル乱数が生成される度に前記レジスターに順次パラレル乱数を保持し、かつ、読出しクロック信号に応じて前記レジスターからパラレル乱数を読み出して出力するとともに、読み出しの終了したレジスターに他のレジスターからパラレル乱数をシフトさせて内容を逐次更新する制御回路を備えたことを特徴とする物理乱数発生装置。

【００４３】

（付記２）前記物理乱数発生器が、複数個のレジスターのうちパラレル乱数を保持すべきレジスターを決めて書き込みアドレスを出力するアップ／ダウンカウンターを備え、前記アップ／ダウンカウンターが出力した書き込みアドレスに基づき、パラレル乱数を保持すべきレジスターを選択してロード信号を出力するセレクターを備え、前記セレクターからのロード信号に基づいて前記シリアル／パラレル変換部内のパラレル乱数を前記レジスターのうち後段のレジスターから前段のレジスターへ順次保持し、かつ、読出しクロック信号に応じて前記レジスターのうち最後段からパラレル乱数を読み出して出力するとともに、このレジスターより前段にある各レジスター内のパラレル乱数を後段へ順次シフトする制御回路を備えたことを特徴とする請求項１に記載の物理乱数発生装置。

【００４４】

（付記３）前記物理乱数発生器が、前記シリアル物理乱数発生器が生成したシリアル乱数の総数をカウントする総数カウンターを備え、前記総数カウンターがカウントしたシリアル乱数の総数が所定のビット数に達したとき、これらのシリアル乱数に基づいてその一様性を検証する乱数検証回路を備えたことを特徴とする請求項１または請求項２に記載の物理乱数発生装置。

【００４５】

（付記４）付記１～３に記載の物理乱数発生装置において、乱数生成用の基準クロックと読出しクロックのいずれか一方または双方に遅延回路または波形成形回路を付加してクロックのエッジを抽出して基準クロックのエッジに対する読出しクロックのエッジの禁止域を最小にするようにしたことを特徴とする物理乱数発生装置。

【００４６】

（付記５）前記乱数検証回路の乱数検証方法として、乱数値“０”または“１”の出現度数をカウントし、これを規定値と比較することによって乱数の一様性を検証する乱数検証方法を採用したことを特徴とする請求項３に記載の物理乱数発生装置。

【００４７】

（付記６）前記乱数検証回路の乱数検証方法として、４ビットで一つの乱数値とし、各々の乱数値の出現度数に基づいて算出されたχ二乗値を規定値と比較することによって乱数の一様性を検証する乱数検証方法を採用したことを特徴とする請求項３に記載の物理乱数発生装置。

【００４８】

（付記７）前記乱数検証回路の乱数検証方法として、連の長さ別にその出現度数をカウントし、これらを規定値と比較することによって乱数の一様性を検証する乱数検証方法を採用したことを特徴とする請求項３に記載の物理乱数発生装置。

【００４９】

（付記８）前記乱数検証回路の乱数検証方法として、所定ビット数の乱数中に出現した最長の連の長さを規定値と比較することによって乱数の一様性を検証する乱数検証方法を採用したことを特徴とする請求項３に記載の物理乱数発生装置。

【００５０】

（付記９）チップセレクトと出力イネーブル機能とそれに対応した端子を備え、出力部のバッファー機能を３ステートとしたことを特徴とする請求項１から請求項７までのいずれかに記載の物理乱数発生装置。

【００５１】

（付記１０）付記９に記載の物理乱数発生装置において、第１セレクター、カウンターを有して選択信号（A0＝“０”、A1＝“１”）の時には乱数検証状態とモニターアドレスを出力し、選択信号（A0＝“１”、A1＝“１”）の時には乱数の判定結果と検証データを出力し、読出しクロックでモニターアドレスの更新を行なうようにしたことを特徴とする物理乱数発生装置。

【００５２】

（付記１１）付記１０に記載の物理乱数発生装置において、一様性乱数のPokerTestの度数分布データを出力するようにしたことを特徴とする物理乱数発生装置。

【００５３】

（付記１２）付記９～１１に記載の物理乱数発生装置において、読出しクロックにて一様性乱数検証のスタート時にパラレル乱数の保持に関連した回路（カウン

ター、シフトレジスター、アップ／ダウンカウンター、レジスター）の初期化を行い、すべての保持されたパラレル乱数が一様性乱数の検証済みの乱数を出力するようにしたことを特徴とする物理乱数発生装置。

【００５４】

（付記１３）前記物理乱数発生器を複数個用意し、セレクターのセレクト信号に基づき、前記物理乱数発生器の中から一つを選択して乱数または乱数検証データを出力することを特徴とする請求項１から請求項８までのいずれかに記載の物理乱数発生装置。

【００５５】

【発明の効果】

以上説明したように、本発明のうち請求項１～７に係る発明によれば、生成された物理乱数を効率よく利用することができるとともに、その乱数の一様性を容易に検定して使用することができ、かつ、簡単な回路構成によりこれらを実現することが可能となる。

【００５６】

また、本発明のうち請求項８、９に係る発明によれば、複数個の物理乱数発生ＩＣを用いて高速に乱数を発生させることが容易となり、かつ、Data Busに直接接続できるようになるため、物理乱数発生装置の使いやすさが格段に向上する。

【図面の簡単な説明】

【図１】

本発明に係る物理乱数発生装置の第１の実施形態を示す回路図である。

【図２】

図１に示す物理乱数発生装置の物理乱数発生器の詳細を示す回路図である。

【図３】

図２に示す物理乱数発生器の各部の出力波形を示す波形図である。

【図４】

図２に示す物理乱数発生器の各部の出力波形を示す波形図である。

【図５】

図１に示す物理乱数発生装置の乱数検証回路のMonobitTestに関する部分の回

路図である。

【図６】

図１に示す物理乱数発生装置の乱数検証回路のPokerTestに関する部分の回路図である。

【図７】

図１に示す物理乱数発生装置の乱数検証回路のRunsTestに関する部分の回路図である。

【図８】

図１に示す物理乱数発生装置の乱数検証回路のRunsTestに関する部分の回路図である。

【図９】

図１に示す物理乱数発生装置の乱数検証回路のLongRunsTestに関する部分の回路図である。

【図１０】

本発明に係る物理乱数発生装置の第２の実施形態を示す回路図である。

【図１１】

本発明に係る物理乱数発生装置の第３の実施形態を示す回路図である。

【図１２】

図１１に示す物理乱数発生装置の各部の出力波形を示す波形図である。

【符号の説明】

１……物理乱数発生器

２……シリアル物理乱数発生器

４……シリアル／パラレル変換部（シフトレジスター）

５……レジスター

６……制御回路

７……アップ／ダウンカウンター

８、１２……セレクター

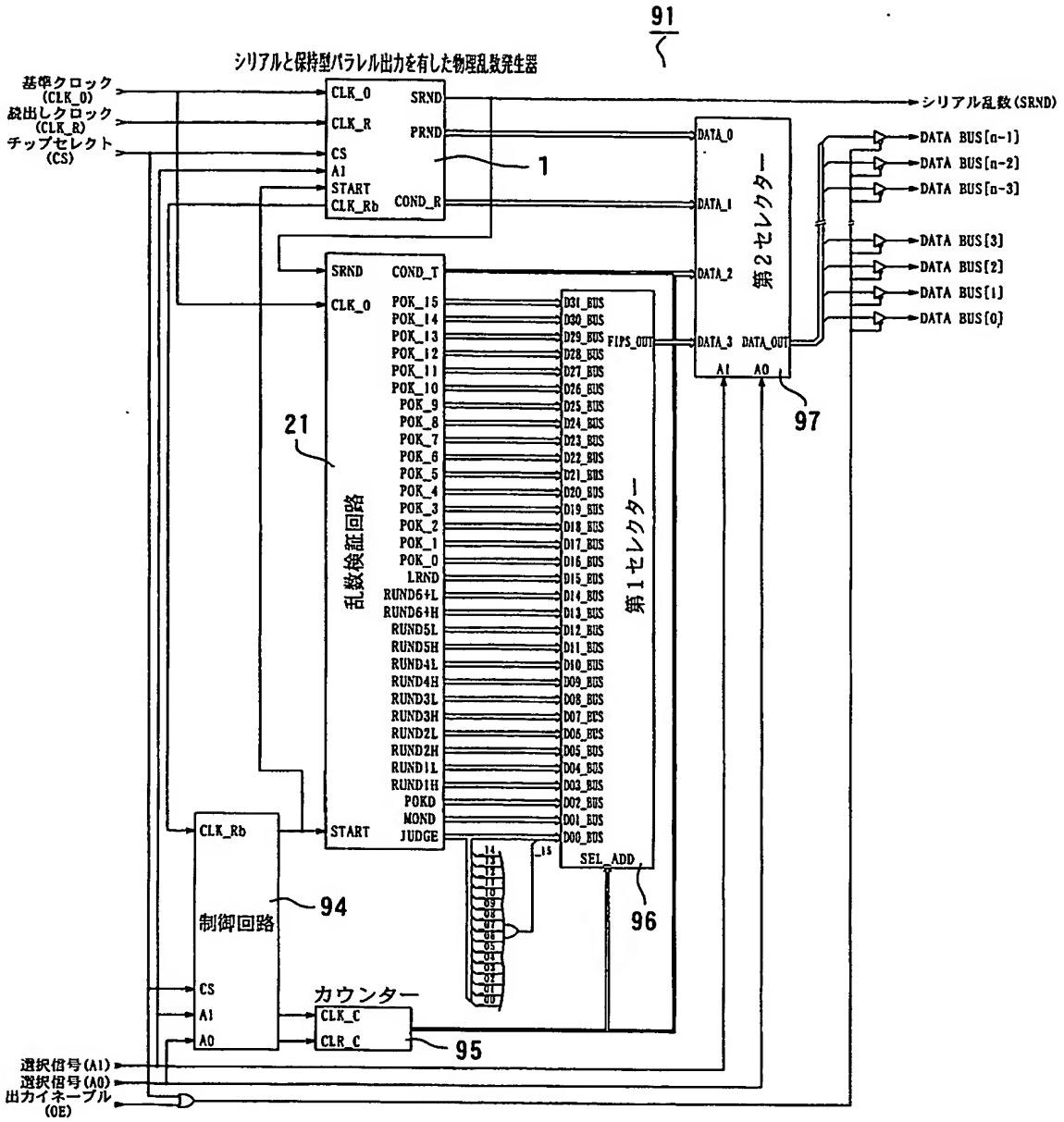
２３、３３、５３、７３……総数カウンター（第１カウンター）

２６、３７、５７、７６……乱数検証回路（制御回路）

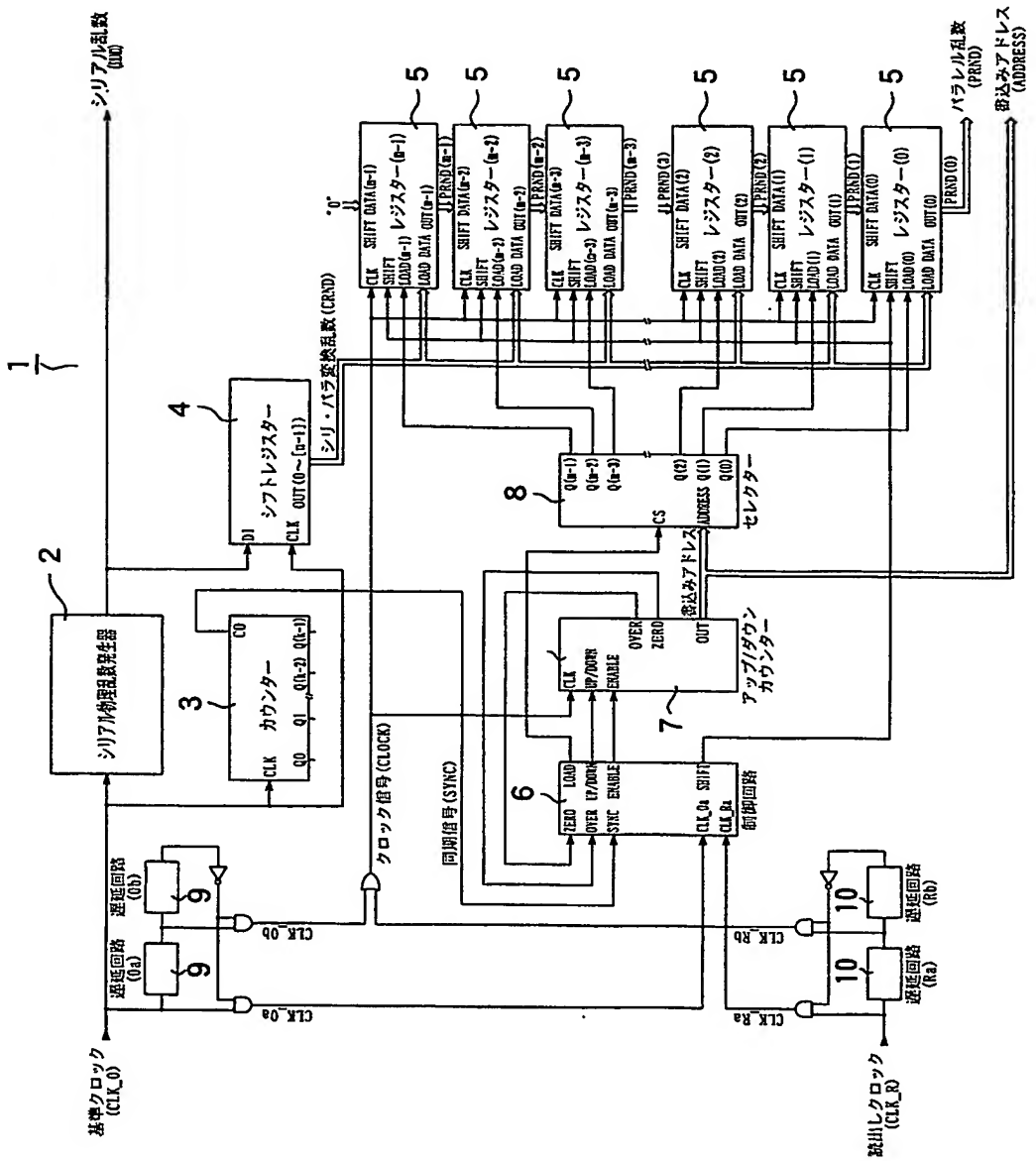
９１……物理乱数発生装置

【書類名】　図面

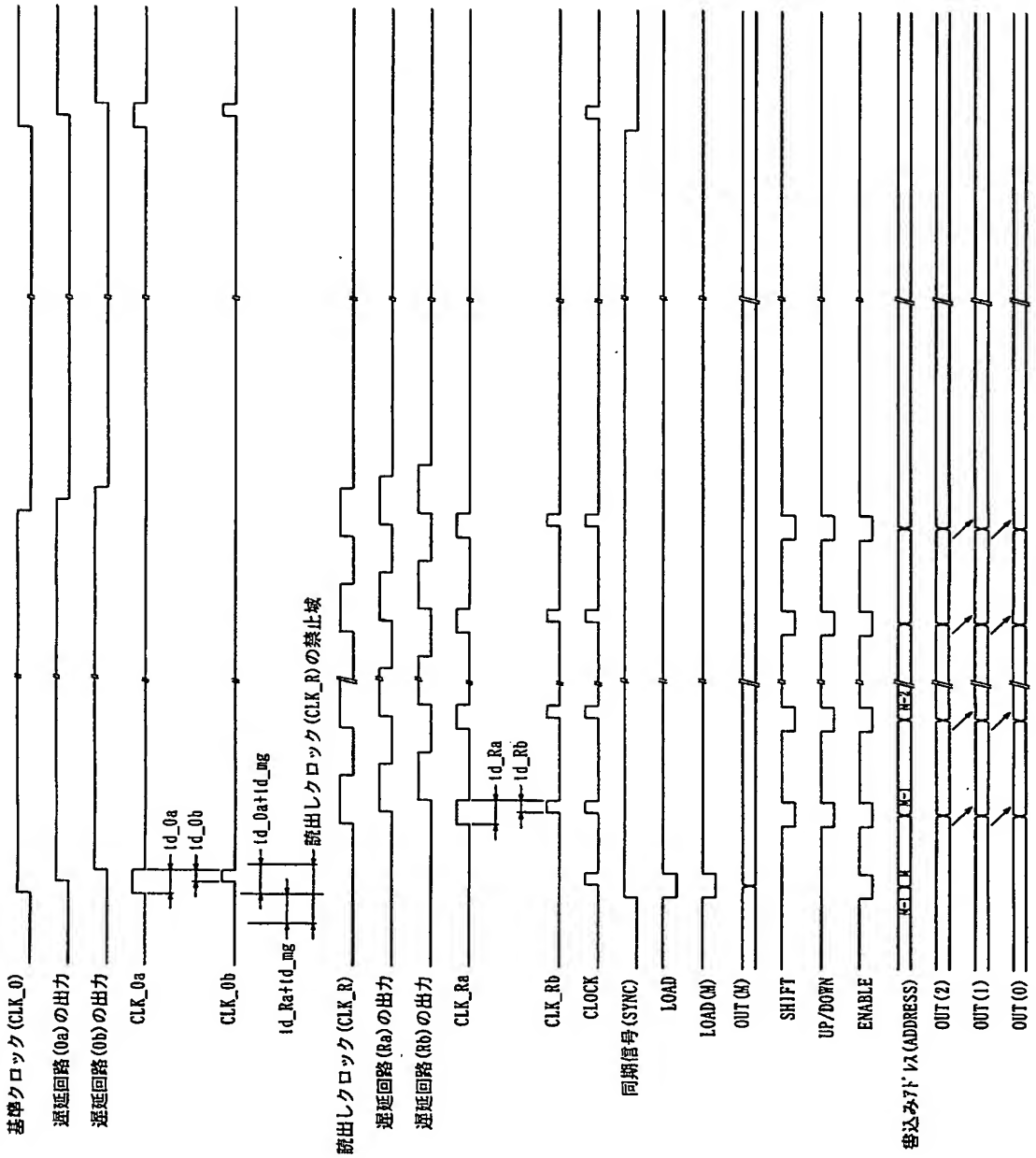
【図１】


91
シリアルと保持型パラレル出力を有した物理乱数発生器
基準クロック (CLK_0)
読出しクロック (CLK_R)
チップセレクト (CS)
CLK_0
CLK_R
CS
A1
START
CLK_Rb
SRND
PRND
COND_R
1
シリアル乱数(SRND)
DATA_0
DATA_1
DATA_2
DATA_3
DATA_OUT
第２セレクター
A1
A0
97
DATA BUS[n-1]
DATA BUS[n-2]
DATA BUS[n-3]
DATA BUS[3]
DATA BUS[2]
DATA BUS[1]
DATA BUS[0]
SRND
CLK_0
COND_T
POK_15
POK_14
POK_13
POK_12
POK_11
POK_10
POK_9
POK_8
POK_7
POK_6
POK_5
POK_4
POK_3
POK_2
POK_1
POK_0
LRND
RUND6+L
RUND6+H
RUND5L
RUND5H
RUND4L
RUND4H
RUND3L
RUND3H
RUND2L
RUND2H
RUND1L
RUND1H
POKD
MOND
JUDGE
START
21
乱数検証回路
D31_BUS
D30_BUS
D29_BUS
D28_BUS
D27_BUS
D26_BUS
D25_BUS
D24_BUS
D23_BUS
D22_BUS
D21_BUS
D20_BUS
D19_BUS
D18_BUS
D17_BUS
D16_BUS
D15_BUS
D14_BUS
D13_BUS
D12_BUS
D11_BUS
D10_BUS
D09_BUS
D08_BUS
D07_BUS
D06_BUS
D05_BUS
D04_BUS
D03_BUS
D02_BUS
D01_BUS
D00_BUS
FIPS_OUT
SEL_ADD
第１セレクター
96
CLK_Rb
制御回路
94
CS
A1
A0
カウンター
CLK_C
CLR_C
95
選択信号(A1)
選択信号(A0)
出力イネーブル (OE)

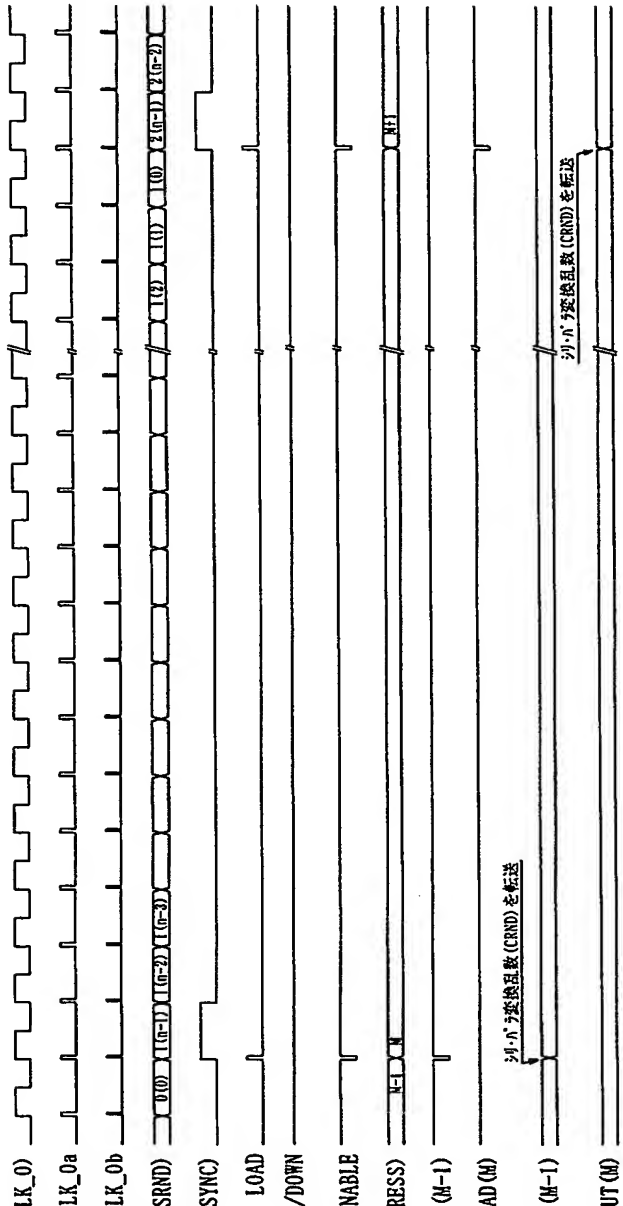
【図２】


1
2
3
4
5
6
7
8
9
10
シリアル乱数 (DIN)
パラレル乱数 (PRND)
書込みアドレス (ADDRESS)
シリアル外部乱数発生器
カウンター
シフトレジスター
シリ・パラ変換乱数 (CRND)
レジスター
セレクター
アップ/ダウン カウンター
制御回路
クロック信号 (CLOCK)
同期信号 (SYNC)
遅延回路 (Ra)
遅延回路 (Rb)
遅延回路 (Oa)
遅延回路 (Ob)
基準クロック (CLK_O)
読出しクロック (CLK_R)

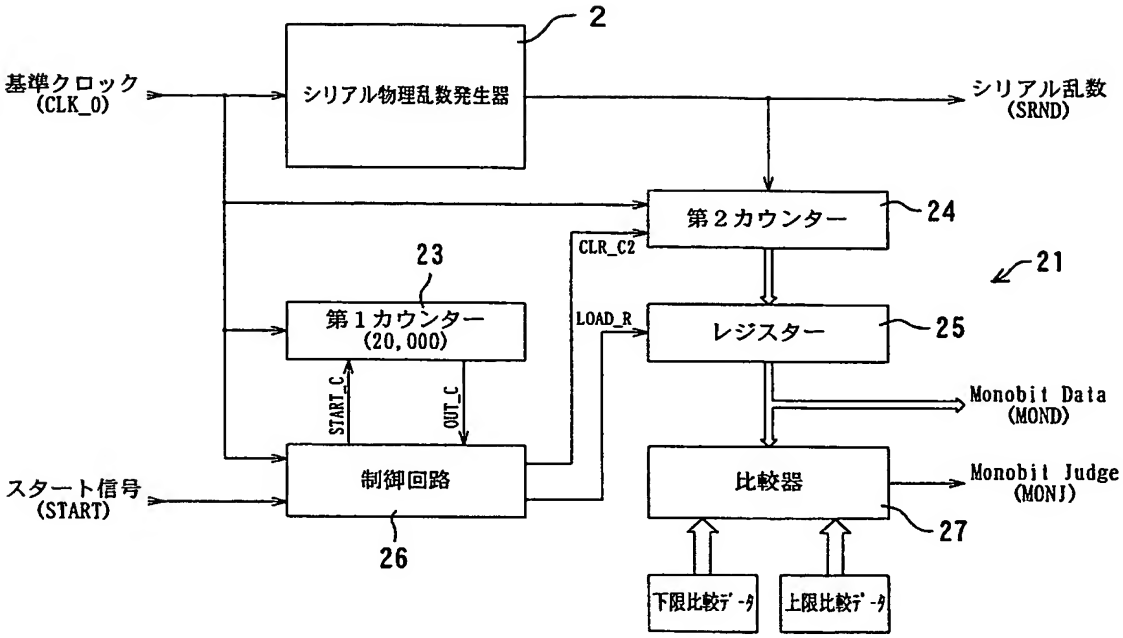
【図３】


基準クロック(CLK_0)
遅延回路(0a)の出力
遅延回路(0b)の出力
CLK_0a
Id_0a
Id_0b
CLK_0b
Id_0a+Id_mg
Id_Ra+Id_mg
読出しクロック(CLK_R)の禁止域
読出しクロック(CLK_R)
遅延回路(Ra)の出力
遅延回路(Rb)の出力
CLK_Ra
Id_Ra
Id_Rb
CLK_Rb
CLOCK
同期信号(SYNC)
LOAD
LOAD(M)
OUT(M)
SHIFT
UP/DOWN
ENABLE
書込みアドレス(ADDRESS)
OUT(2)
OUT(1)
OUT(0)

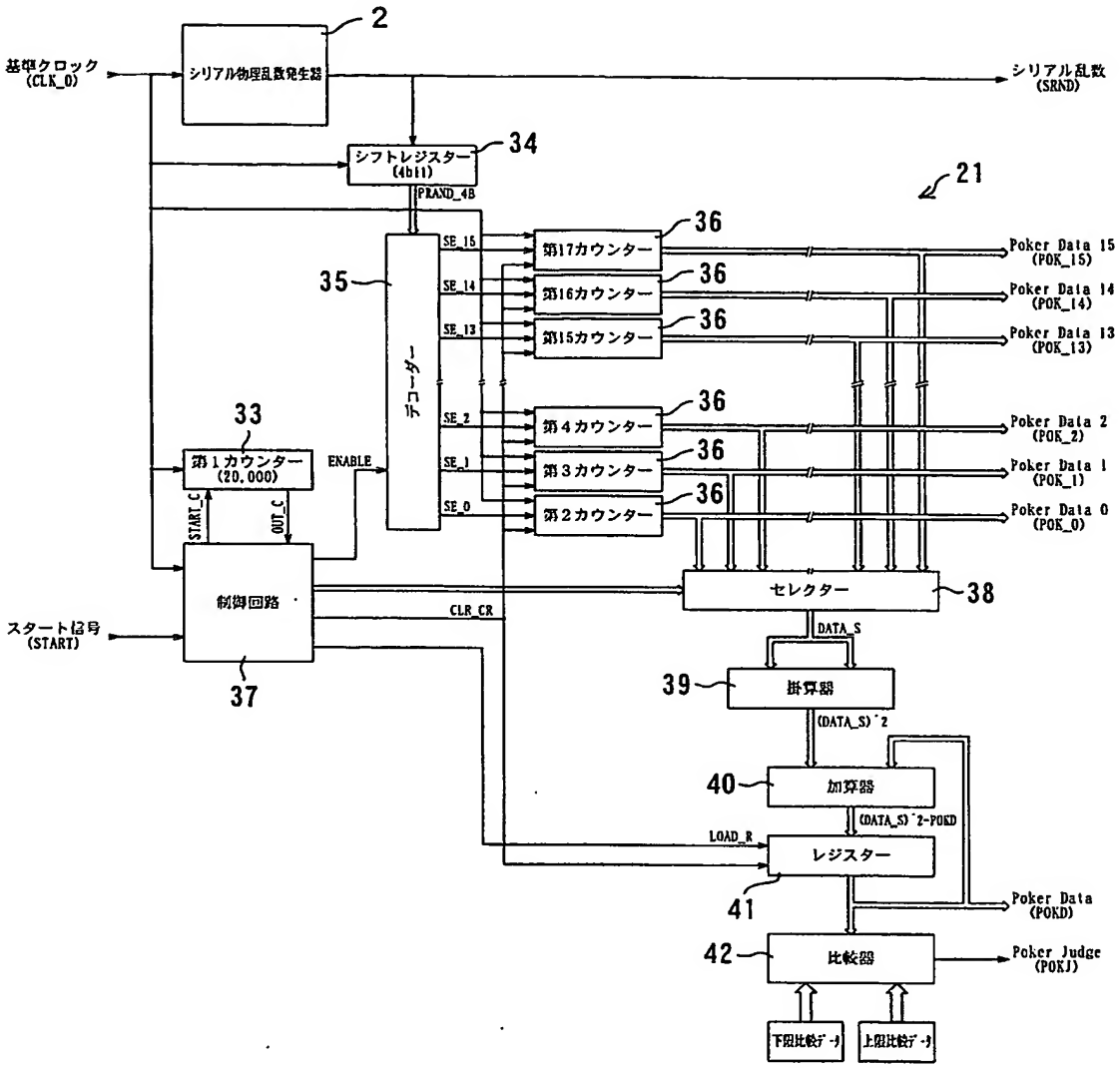
【図４】


基準クロック(CLK_0)
CLK_0a
CLK_0b
シリアル乱数(SRND)
同期信号(SYNC)
LOAD
UP/DOWN
ENABLE
書込みアドレス(ADDRESS)
LOAD(M-1)
LOAD(M)
OUT(M-1)
OUT(M)
M-1
M
M+1
シリアル乱数(CRND)を転送
シリアル乱数(CRND)を転送

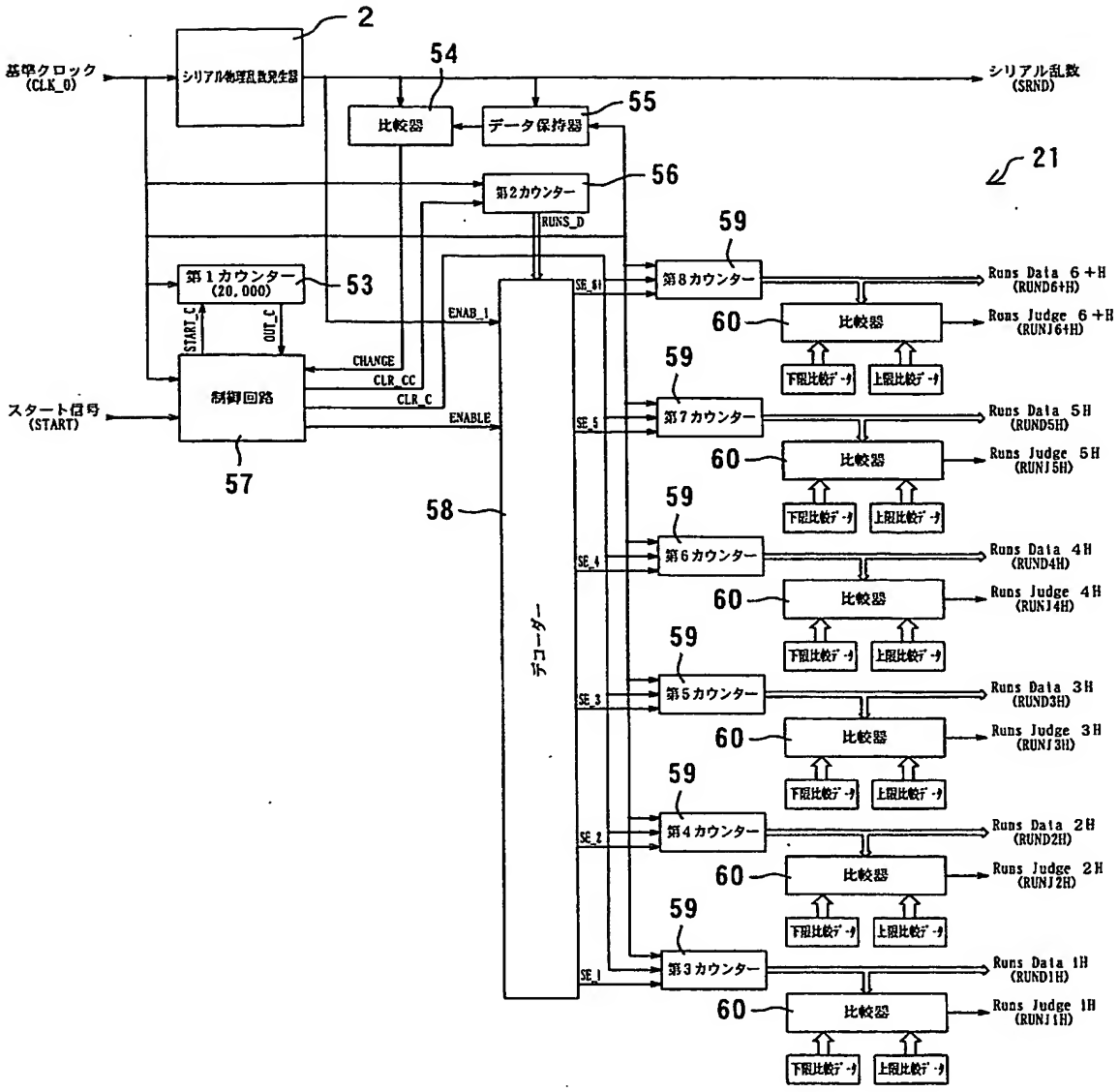
【図５】


2
基準クロック
(CLK_0)
シリアル物理乱数発生器
シリアル乱数
(SRND)
第２カウンター
24
CLR_C2
21
23
第１カウンター
(20,000)
LOAD_R
レジスター
25
START_C
OUT_C
Monobit Data
(MOND)
スタート信号
(START)
制御回路
比較器
Monobit Judge
(MONJ)
27
26
下限比較ﾃﾞｰﾀ
上限比較ﾃﾞｰﾀ

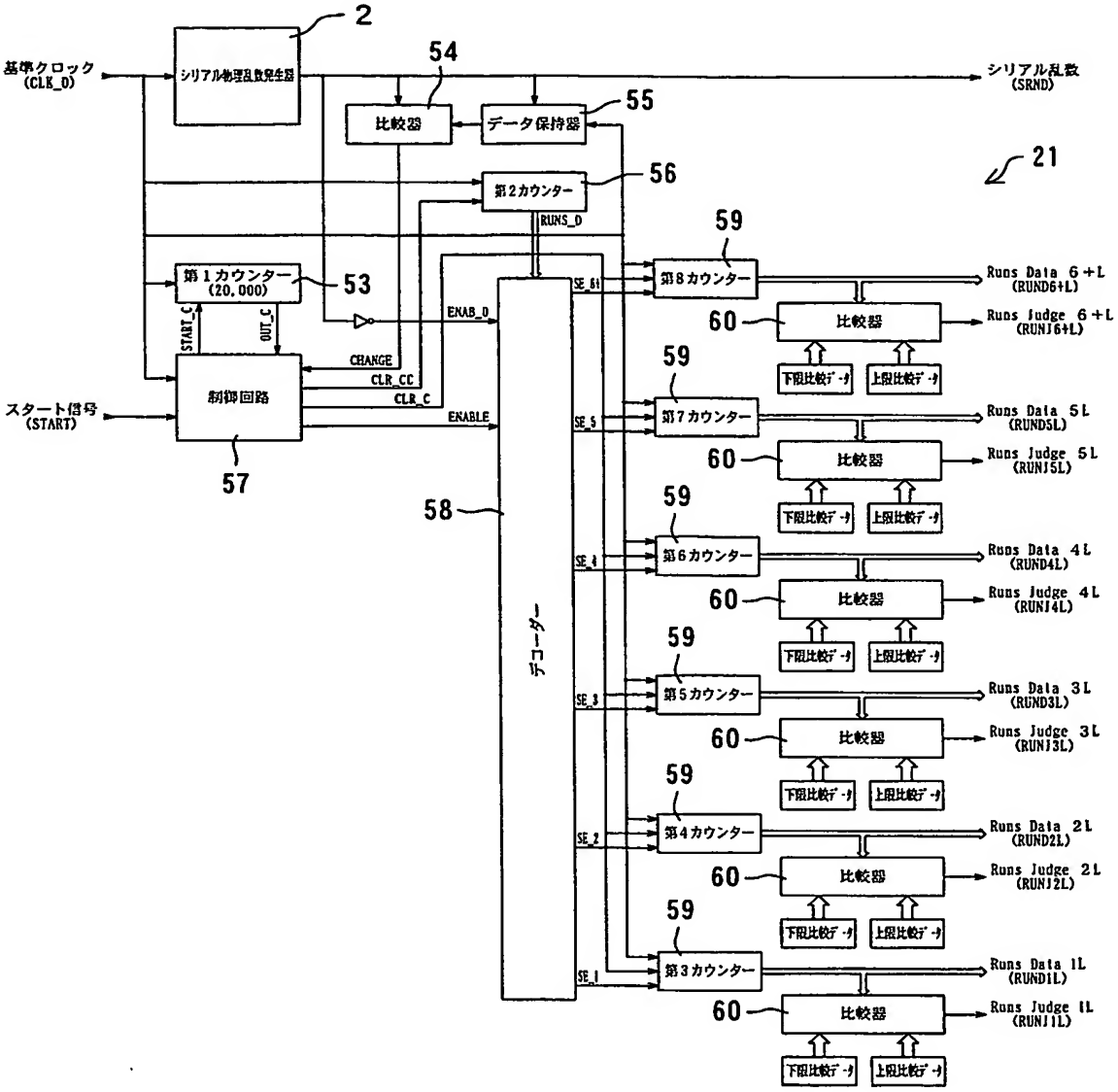
【図６】


2
基準クロック
(CLK_0)
シリアル物理乱数発生器
シリアル乱数
(SRND)
シフトレジスター
(4bit)
34
PRAND_4B
21
36
35
SE_15
SE_14
SE_13
SE_2
SE_1
SE_0
デコーダー
第17カウンター
第16カウンター
第15カウンター
第4カウンター
第3カウンター
第2カウンター
Poker Data 15
(POK_15)
Poker Data 14
(POK_14)
Poker Data 13
(POK_13)
Poker Data 2
(POK_2)
Poker Data 1
(POK_1)
Poker Data 0
(POK_0)
33
第1カウンター
(20,000)
ENABLE
START_C
OUT_C
制御回路
スタート信号
(START)
37
CLR_CR
セレクター
38
DATA_S
39
掛算器
(DATA_S)*2
40
加算器
(DATA_S)*2-POKD
LOAD_R
レジスター
41
Poker Data
(POKD)
42
比較器
Poker Judge
(POKJ)
下限比較データ
上限比較データ

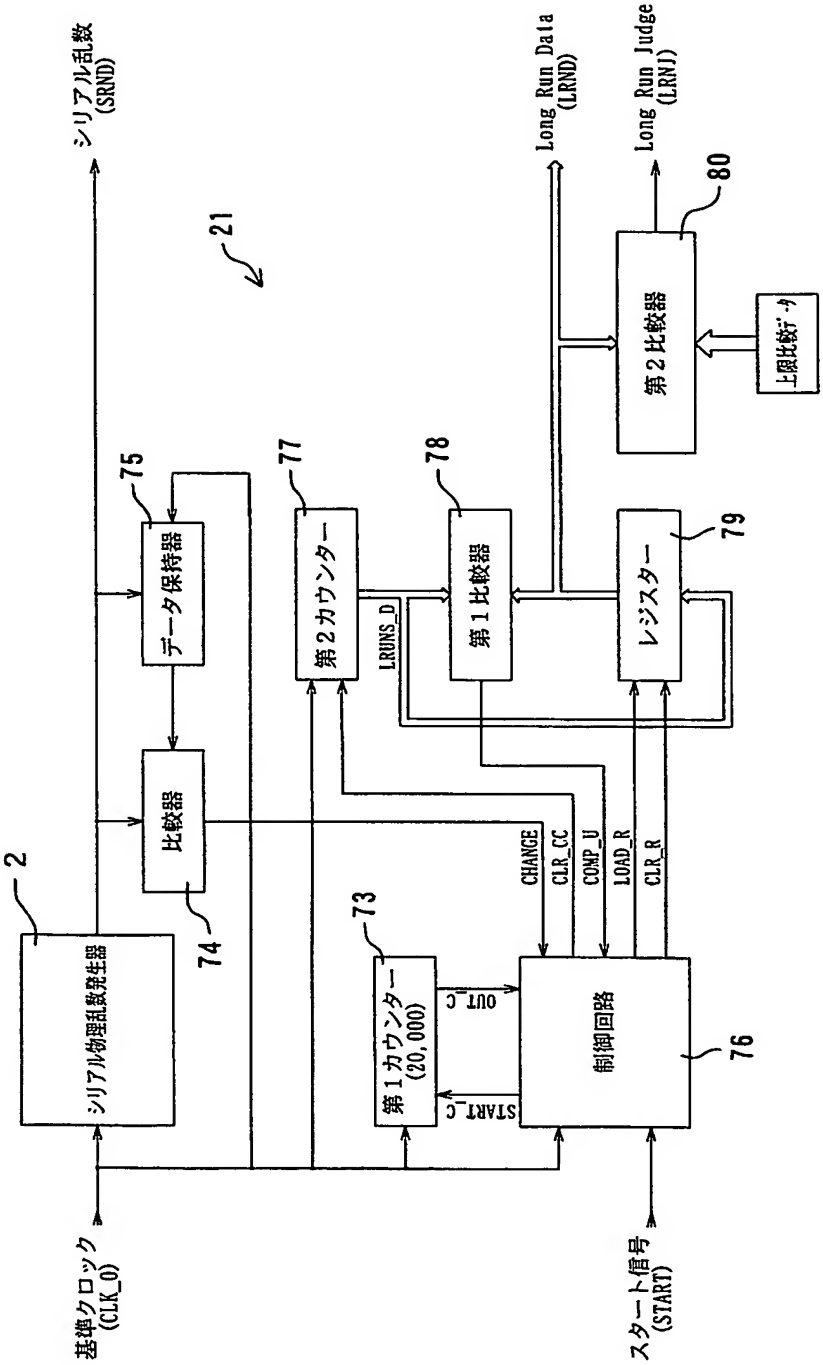
【図７】


2
基準クロック
(CLK_0)
シリアル物理乱数発生器
シリアル乱数
(SRND)
54
比較器
55
データ保持器
21
56
第2カウンター
RUNS_D
59
第1カウンター
(20,000)
53
第8カウンター
Runs Data 6+H
(RUND6+H)
60
比較器
Runs Judge 6+H
(RUNJ6+H)
下限比較データ
上限比較データ
START_C
OUT_C
ENAB_1
CHANGE
CLR_CC
CLR_C
ENABLE
制御回路
スタート信号
(START)
57
SE_6
SE_5
SE_4
SE_3
SE_2
SE_1
58
デコーダー
第7カウンター
Runs Data 5H
(RUND5H)
Runs Judge 5H
(RUNJ5H)
第6カウンター
Runs Data 4H
(RUND4H)
Runs Judge 4H
(RUNJ4H)
第5カウンター
Runs Data 3H
(RUND3H)
Runs Judge 3H
(RUNJ3H)
第4カウンター
Runs Data 2H
(RUND2H)
Runs Judge 2H
(RUNJ2H)
第3カウンター
Runs Data 1H
(RUND1H)
Runs Judge 1H
(RUNJ1H)

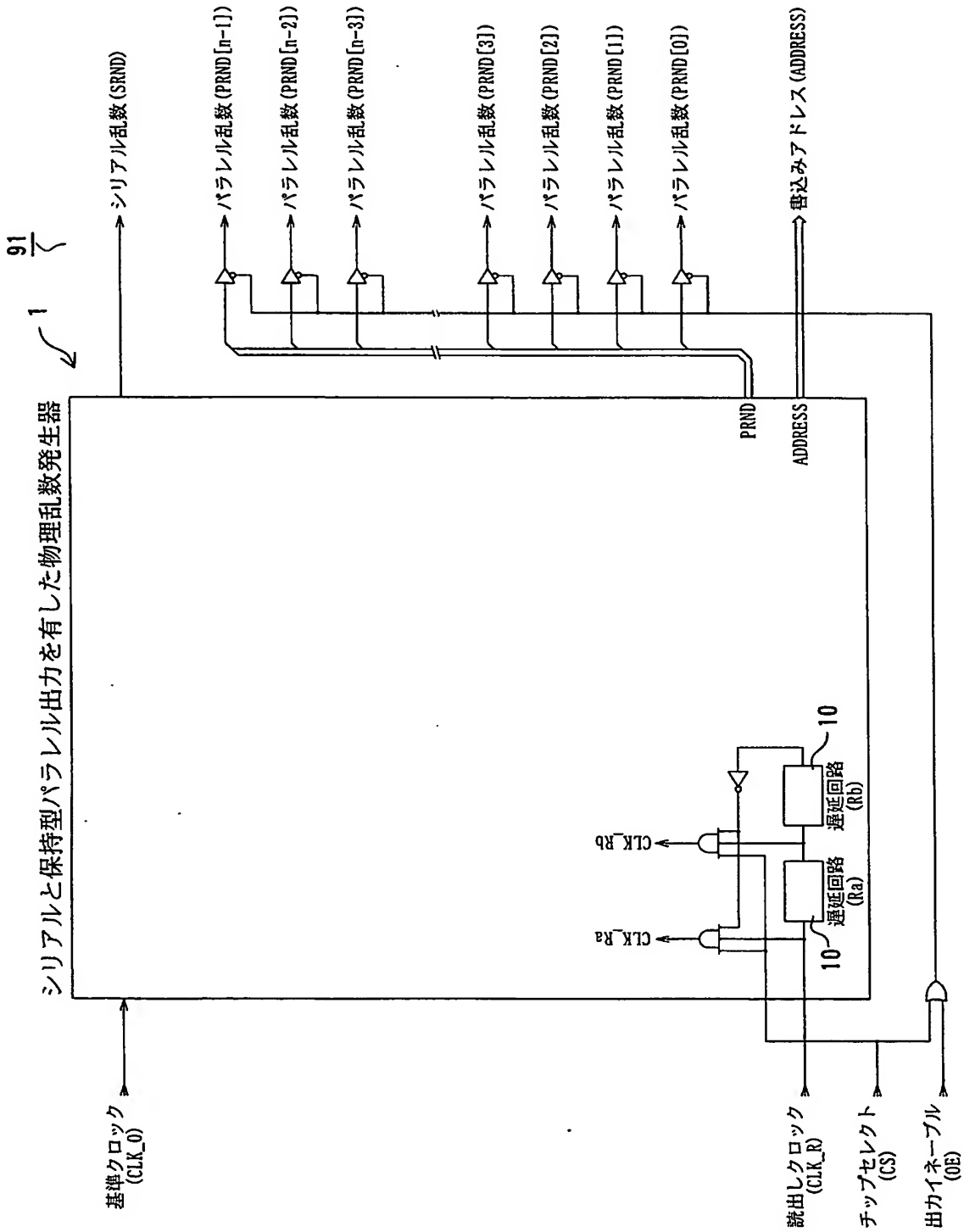
【図８】


2
54
55
56
21
59
53
57
58
60
基準クロック
(CLK_0)
シリアル物理乱数発生器
シリアル乱数
(SRND)
比較器
データ保持器
第２カウンター
RUNS_D
第１カウンター
(20,000)
START_C
OUT_C
CHANGE
CLR_CC
CLR_C
ENAB_D
ENABLE
制御回路
スタート信号
(START)
デコーダー
SE_8
SE_7
SE_6
SE_5
SE_4
SE_3
SE_2
SE_1
第８カウンター
第７カウンター
第６カウンター
第５カウンター
第４カウンター
第３カウンター
Runs Data 6+L
(RUND6+L)
Runs Judge 6+L
(RUNJ6+L)
Runs Data 5L
(RUND5L)
Runs Judge 5L
(RUNJ5L)
Runs Data 4L
(RUND4L)
Runs Judge 4L
(RUNJ4L)
Runs Data 3L
(RUND3L)
Runs Judge 3L
(RUNJ3L)
Runs Data 2L
(RUND2L)
Runs Judge 2L
(RUNJ2L)
Runs Data 1L
(RUND1L)
Runs Judge 1L
(RUNJ1L)
下段比較データ
上段比較データ

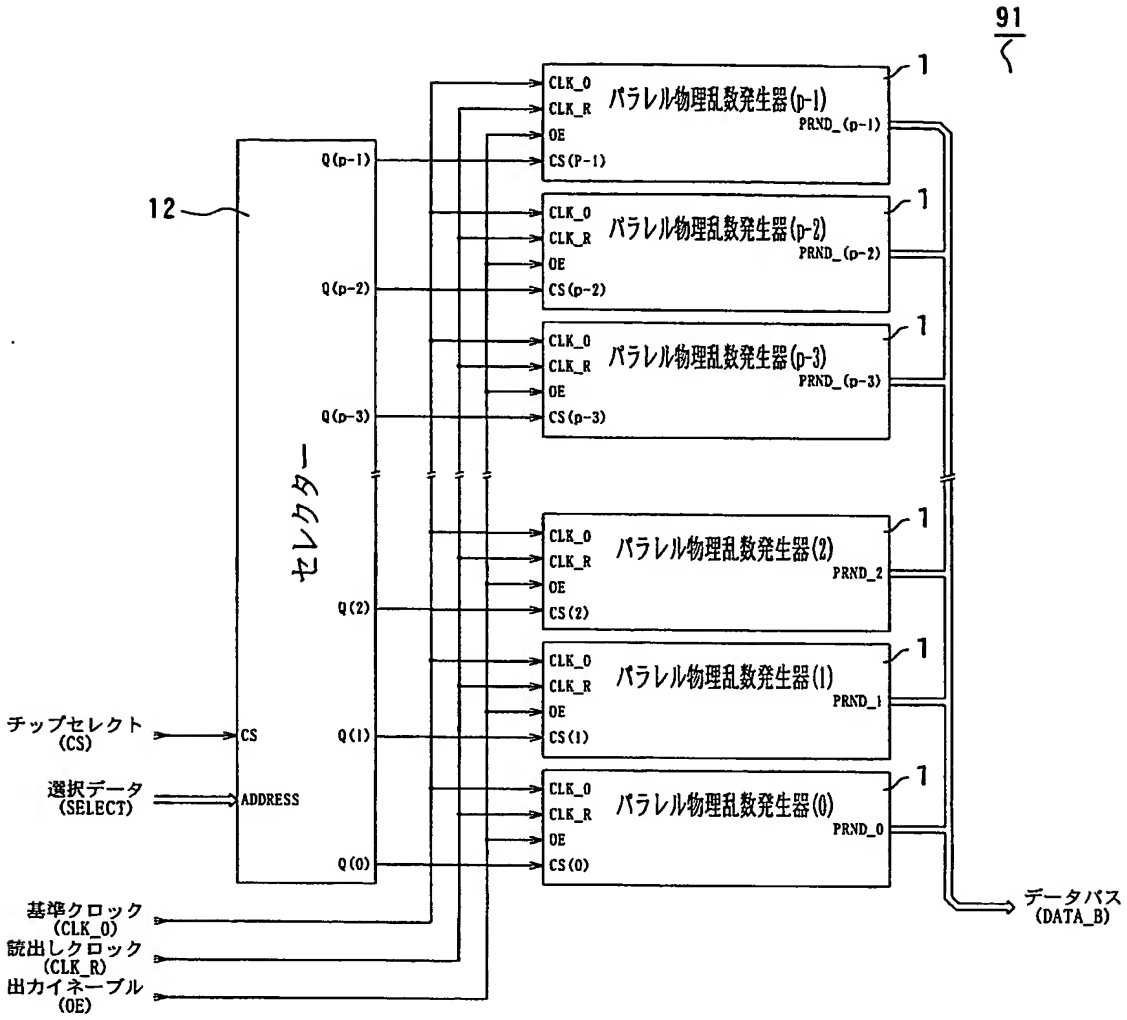
【図９】


シリアル乱数
(SRND)
Long Run Data
(LRND)
Long Run Judge
(LRNJ)
21
80
第２比較器
上限比較データ
75
77
78
データ保持器
第２カウンター
第１比較器
79
レジスター
LRUNS_D
2
比較器
CHANGE
CLR_CC
COMP_U
LOAD_R
CLR_R
74
73
シリアル物理乱数発生器
第１カウンター
(20,000)
OUT
START
制御回路
76
基準クロック
(CLK_0)
スタート信号
(START)

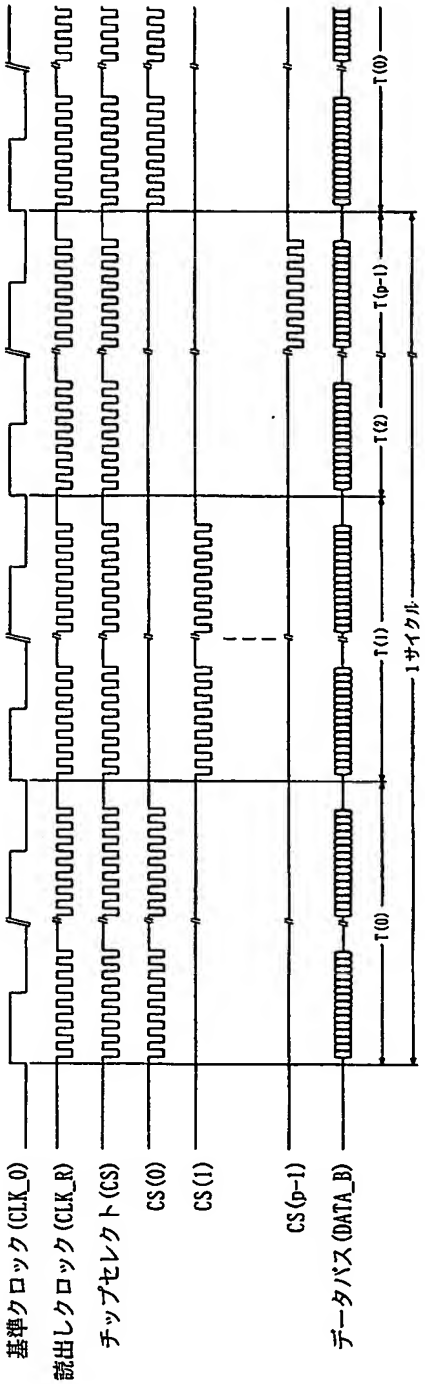
【図１０】


91
1
シリアル乱数(SRND)
パラレル乱数(PRND[n-1])
パラレル乱数(PRND[n-2])
パラレル乱数(PRND[n-3])
パラレル乱数(PRND[3])
パラレル乱数(PRND[2])
パラレル乱数(PRND[1])
パラレル乱数(PRND[0])
書込みアドレス(ADDRESS)
シリアルと保持型パラレル出力を有した物理乱数発生器
PRND
ADDRESS
10
遅延回路(Rb)
遅延回路(Ra)
10
CLK_Rb
CLK_Ra
基準クロック(CLK_0)
読出しクロック(CLK_R)
チップセレクト(CS)
出カイネーブル(OE)

【図１１】


91
12
セレクター
Q(p-1)
Q(p-2)
Q(p-3)
Q(2)
Q(1)
Q(0)
CS
ADDRESS
チップセレクト (CS)
選択データ (SELECT)
基準クロック (CLK_0)
読出しクロック (CLK_R)
出力イネーブル (OE)
CLK_0
CLK_R
OE
CS(P-1)
CS(p-2)
CS(p-3)
CS(2)
CS(1)
CS(0)
パラレル物理乱数発生器(p-1)
パラレル物理乱数発生器(p-2)
パラレル物理乱数発生器(p-3)
パラレル物理乱数発生器(2)
パラレル物理乱数発生器(1)
パラレル物理乱数発生器(0)
PRND_(p-1)
PRND_(p-2)
PRND_(p-3)
PRND_2
PRND_1
PRND_0
1
データバス (DATA_B)

【図１２】


基準クロック(CLK_0)
読出しクロック(CLK_R)
チップセレクト(CS)
CS(0)
CS(1)
CS(p-1)
データバス(DATA_B)
T(0)
T(1)
T(2)
T(p-1)
T(0)
1サイクル

【書類名】　要約書

【要約】

【課題】　セキュリティーなどの用途に用いる物理乱数発生装置において、単体での乱数利用効率を高め、複数の物理乱数ＩＣを組み上げて乱数を高速に発生させ、乱数の質を容易に確認できるようにする。

【解決手段】　物理乱数発生器１を有する物理乱数発生装置であって、物理乱数発生器１が、基準クロック信号に応じてシリアル乱数を生成するシリアル物理乱数発生器２を備える。シリアル乱数をパラレル乱数に変換するシフトレジスター４を備え、パラレル乱数を保持しうる複数個のレジスター５を備える。パラレル乱数が生成される度にレジスター５に順次パラレル乱数を保持し、かつ、読出しクロック信号に応じてレジスター５からパラレル乱数を読み出して出力するとともに、読み出しの終了したレジスター５に他のレジスター５からパラレル乱数をシフトさせて内容を逐次更新する制御回路６を備える。

【選択図】　図２

認定・付加情報

特許出願の番号	特願２００３－１０１０８５
受付番号	５０３００５６２１４８
書類名	特許願
担当官	第八担当上席　　００９７
作成日	平成１５年　４月　７日

＜認定情報・付加情報＞

【提出日】　平成15年 4月 4日

次頁無

特願２００３－１０１０８５

出　願　人　履　歴　情　報

識別番号　　［０００２３７７２１］

１．変更年月日　　２００１年　１月１６日
［変更理由］　　名称変更
住　所　　東京都港区新橋５丁目３６番１１号
氏　名　　エフ・ディー・ケイ株式会社

２．変更年月日　　２００３年　８月１３日
［変更理由］　　名称変更
住　所　　東京都港区新橋５丁目３６番１１号
氏　名　　ＦＤＫ株式会社